REMARKS

Claims 5-11 stand rejected under 35 U.S.C. §102(b) as being anticipated by Tomko (US 5,790,668). This rejection is respectfully traversed on the following grounds.

Applicant largely agrees with the Examiner's description of Tomko's disclosure in paragraph 3. of the official action. Applicant further agrees that Tomko discloses useful techniques for securely storing private information in an electronic database. However, Tomko simply does not teach or suggest the steps of Applicant's claimed invention.

Tomko discloses that fingerprint biometrics of the subscriber and of those employees of the database provider are used to provide security keys. These keys are used to restrict access to the records in the database that contain the subscriber's information. The keys encrypting and decrypt the address of the subscriber's information in the database. See col. 3, line 65 - col. 4, line 7. Nothing in Tomko teaches or suggests that the subscriber's information is itself encrypted with the biometrically-derived security keys. Security of information is maintained essentially because the subscriber's private information is hidden in a difficult-to-identify location within the database structure. The information cannot be found by anyone who does not know the address of the hidden location.

The present invention basically differs from Tomko in that the fingerprint-derived biometrics of the sender and the receiver are used as encryption keys for the actual information being transmitted between sender and receiver. The information transferred between sender and receiver is in encoded form during transmission. The claims call for the private information to be encrypted into a coded form with the sender's

biometric being an essential part of the encryption key. The actual information in encrypted form is transferred to the third-party control system that decrypts information using the sender's biometric-derived key that the control system obtained independently of the transmitted information. Then the control system encrypts the information into a different encrypted form using the receiver's biometric-derived key that the control system has obtained independently. Finally after transmitting the information from the control system in newly encrypted form to the receiver, the information is decrypted by the receiver. These steps are well defined in the claims.

It is thus seen that whenever the information is being transmitted between the authorized parties, namely the sender, receiver and control system, it is in encrypted form. If intercepted, it could not be deciphered without the encryption keys. The information is only in directly-perceptible form when in possession of the authorized parties. In contrast, only the identity of the location of the information within the system database is encrypted according to Tomko. Tomko says nothing to refute that the information remains intact in directly-perceptible form within the database. If so, then an unauthorized intruder theoretically could copy the database as a whole and re-assemble the unencrypted private information by inspection, albeit with difficulty.

Applicant has great respect and admiration for the disclosure of Tomko and does not intend to disparage it in any way. Neither is Applicant promoting its own process as being invincible from attack or otherwise superior to Tomko. These arguments are made to show the differences between Tomko and the present invention.

Tomko and Applicant's novel method also seem tailored to serve different utilities. Tomko is directed primarily to providing access to personal data profiles, such as name, address, digital photo, etc. for example for verifying an individual's entitlement to a welfare benefit. See col. 1, lines 11-20. Thus one of skill in the art contemplates that the private information is stored in a structured database. Moreover, access to the private information is secured effectively by encrypting only the addresses that point to locations of the data profile elements in the database. The present invention is aimed toward the private communication of information between sender and receiver. Thus it emphasizes encryption of the actual information during transfer between the parties.

Although Tomko and the present invention each rely upon fingerprint biometrics for encryption keys related to maintaining the privacy of information, the processes are distinctly different. The plainly specified steps of:

- sender encrypting
- transfer to control
- decrypting by control
- re-encrypting by control
- transfer to receiver, and
- decrypting by receiver

all applied to the actual information being communicated between sender and receiver are neither taught nor suggested by Tomko.

The novel method of securely transmitting information would therefore not have been anticipated or rendered obvious by the cited reference. For the foregoing reasons, Applicant respectfully requests that the rejections be withdrawn and that claims 5-11 be allowed at this time.

Respectfully submitted,

Date: September 27, 2005
2205 Silverside Road
Wilmington DE 19810
Facsimile:(302) 475-7915

Jeffrey C. Lew
Attorney for Applicant
Registration No. 35,935
Telephone:(302) 475-7919